Source of Acquisition
NASA Marshall Space Flight Center

TTTech

Time-Triggered Protocol (TTP) for Integrated Modular Avionics (IMA)

Draft Version
Content to be updated for MAPLD conference presentation

Dr. Guenther Bauer, Dr. Mirko Jakovljevic,
Leonard Gagea, Guenter Motzet
TTTech Computertechnik AG

David A. Gwaltney
NASA

2006 MAPLD International Conference,
Washington, DC

The Integrated Safety-Critical Advanced Avionics Communication & Control (ISAACC) System is the product of the Propulsion High-Impact Avionics Technologies (PHIAT) project at NASA Marshall Space Flight Center (MSFC) during FY03 to the end of FY05

- Originally funded under Next Generation Launch Technologies (NGLT) for four years beginning in mid FY03
- Tasked to develop avionics technologies for control of next generation reusable rocket engines
- Funded under the Exploration Systems Mission Directorate (ESMD) through end of FY05
- Broadened scope to include vehicle systems control for human and robotic missions

The goal is an avionics architecture suitable for control and monitoring of safety critical systems of manned spacecraft

- Scalable to allow its use in robotic vehicles or launch pad and propulsion test stand monitoring and control systems.

Four primary areas of focus for the ISAACC distributed real-time control system to provide a reliable system for human spaceflight, while also providing scalability and addressing cost sensitivity and sustaining engineering.

- Modular components
  - High reusability
  - Flexibility to accommodate upgrades
  - Limit number of unique designs
  - Scalable
- Hard real-time, safety critical communications between modules and systems of modules
  - Fault detection, containment and tolerance
  - High availability, High reliability
  - Guaranteed quality of service – low jitter/latency
- Distributed intelligence
  - Complex functionality using processing elements with moderate capability (i.e. Current Rad Hard processors/FPGAs)
  - Fault Tolerance / Fault Detection, Isolation and Recovery (FDIR)
- Plug-and-Play / Hot Swap at all levels (Modules, Transducers, Controlled Components)
  - Improved maintainability
  - Increased flexibility
  - Reduce cost of software changes / unique software configurations

Federated

- every LRU/ECU has one function only
- Power supply & rugged chassis for every LRU
- Excessive weight, higher system integration hard to accomplish

Integrated Modular Avionics (IMA)

- Common power supply & rugged chassis for a set of modules
- many upgradeable SW functions on one module (i.e. processing unit)
- Reduced weight, straightforward update and system integration
- Partitioning and MMU important!

  Note: MMU=Memory Management Unit

IMA philosophy

- Run many partitioned functions on one embedded computer
- Use shared resources (processing time, I/O, power supply, ...)

Distributed IMA philosophy

- Run many partitioned functions on one distributed fault-tolerant embedded computer
- Share common communication medium

TTP: A Distributed IMA Platform Technology

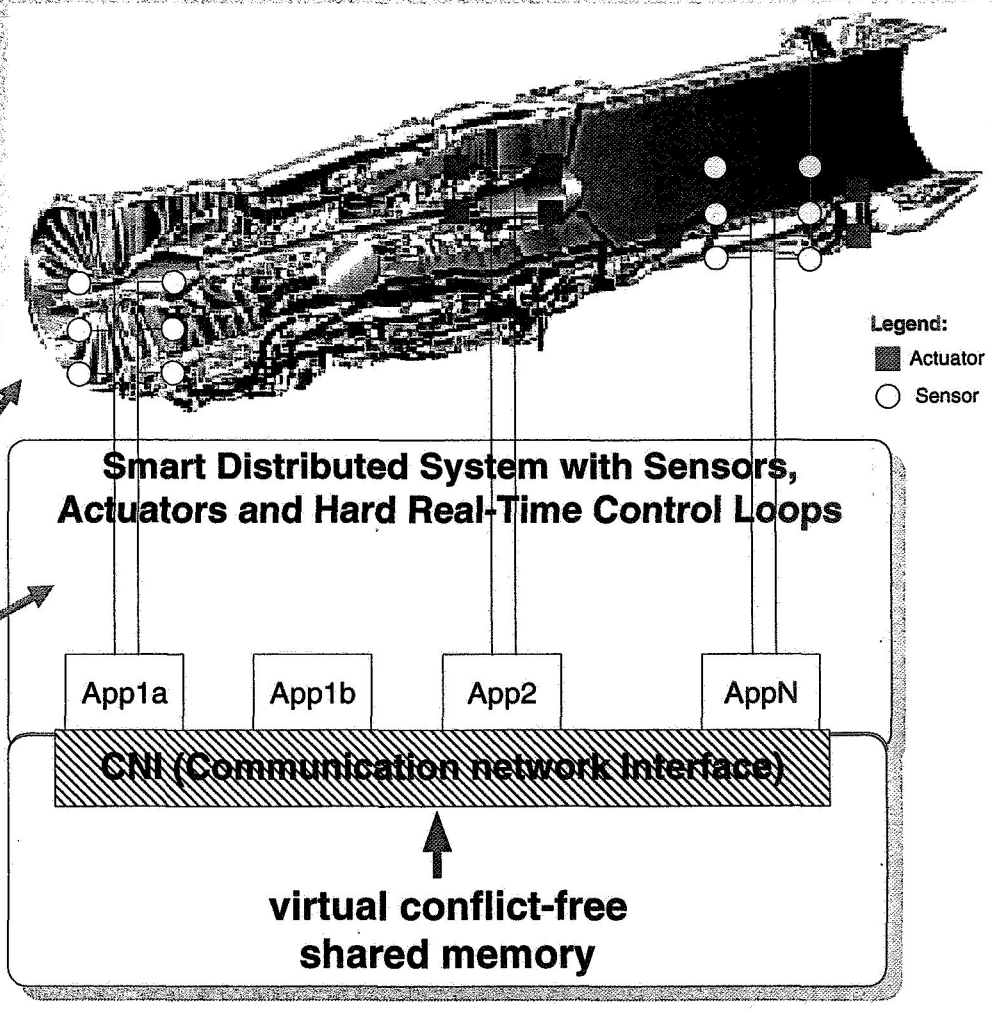
TTTech

"The network is a deterministic fault-tolerant hard real-time embedded computer"

- system architecture with system redundancy and voting
- system health monitoring and high data integrity
- strictly deterministic communication (max. 25MBit/s))
- system synchronization (jitter in µs range)

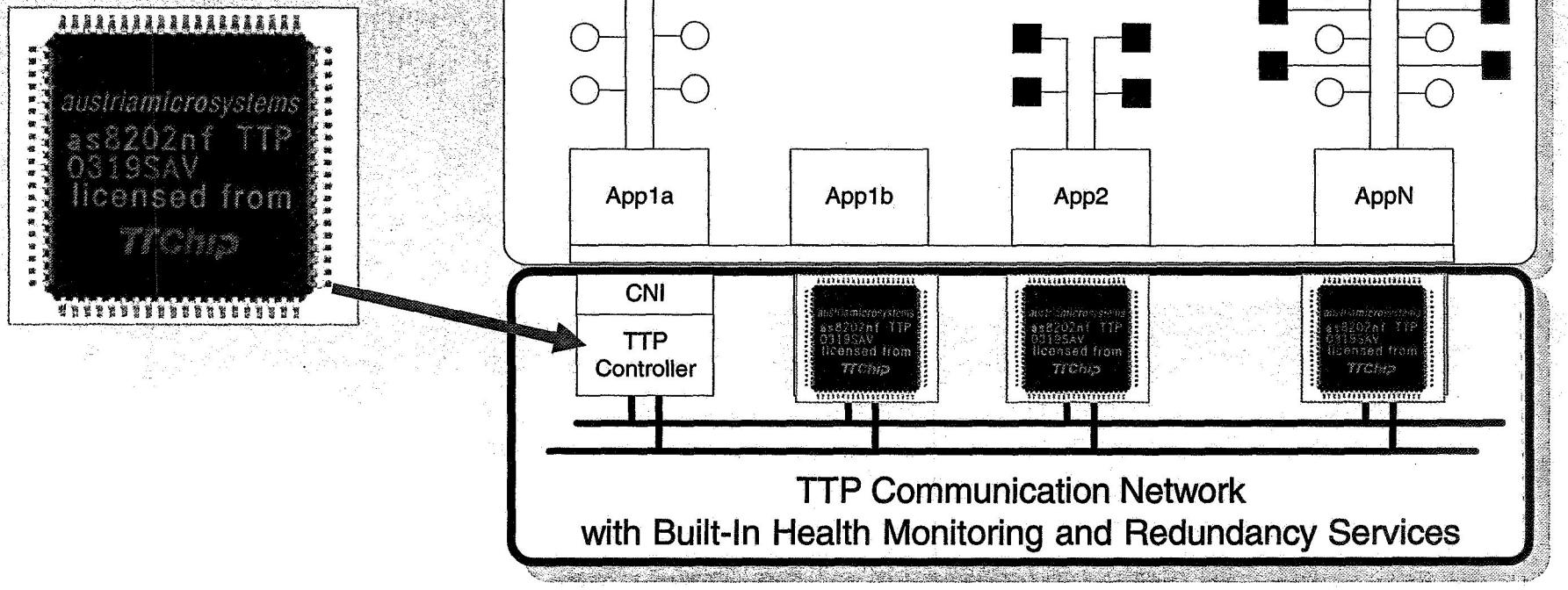
Application designer focused on:

- application-specific issues
- fast real-time control loops



TTP: Built-in Distributed Services

TTTech



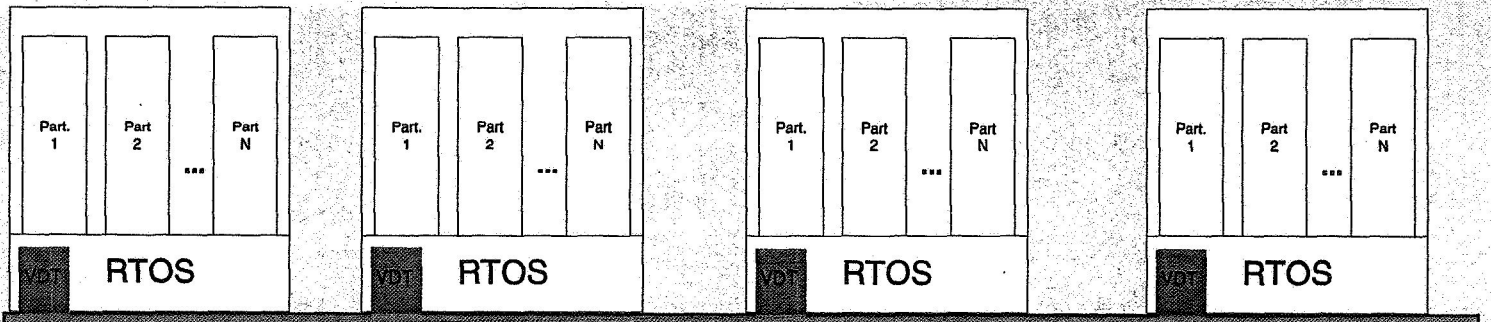
On-chip TTP protocol guarantees autonomous operation of communication system, independent of application host/software:

TTP: Parametric System Design

TTTech

Parametric design of LRU software behavior (RTOS, def. table)

- Standard software application interfaces
- Definition of conflict-free use of shared resources
- Definition of LRUs temporal behavior



TTTech: Parametric system architecture definition (TTP; MEDL)

MEDL

- Definition and tight control of key system interfaces
- Independent of topology, physical layer or distance
- Definition of conflict-free use of system shared resources
- Definition of system temporal behavior

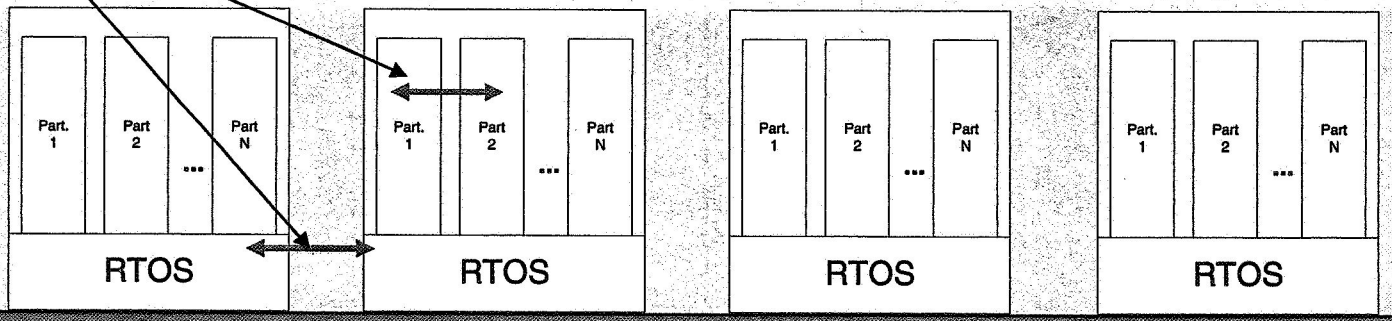
TTP: System (not only LRU SW!) Partitioning

TTTech

Software partitioning using MMU and scheduled resource use

- No fault propagation to other software partitions
- Conflict-free use of shared resources among partitions (I/O, memory, ...)
- MMU may be a weak point -> solution by using one partition per LRU!

Fault Isolation



TTTech: System Partitioning using TDMA and other TTP mechanisms

- No control error propagation to other LRUs after (single) HW or SW fault
- Prevention of timing violations of controller by bus guardian
- Conflict-free use of communication resource among LRUs
- Communication system operates autonomously, based on predefined schedule, distributed network management and fault-tolerant time base

Benefits (I)

TTTech

Reduced (re)design costs

- Simplified design of complex integrated systems
- Reduced upgrade/extension/reconfiguration costs

Reduced integration and system testing costs

- integration provided per default
- no jitters, hazards, coupled temporal/logical effects and fault propagation
- concurrent engineering and separate testing possible!

Simplified design for system autonomy

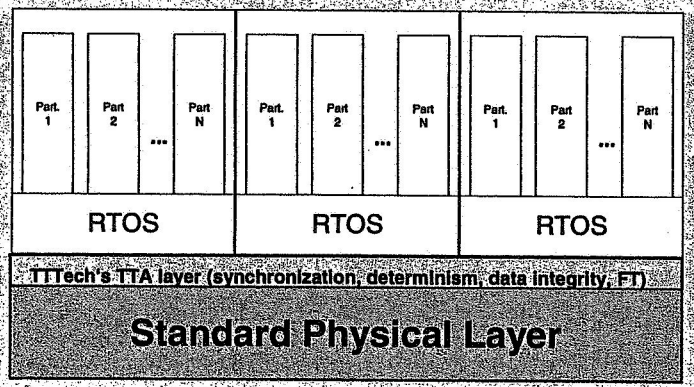
- Improved stability as a result of strict control of key interfaces and system partitioning
- Simplified design of redundant systems and graceful degradation due to the built-in services

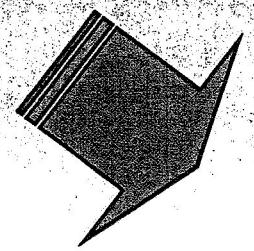
Benefits (II)

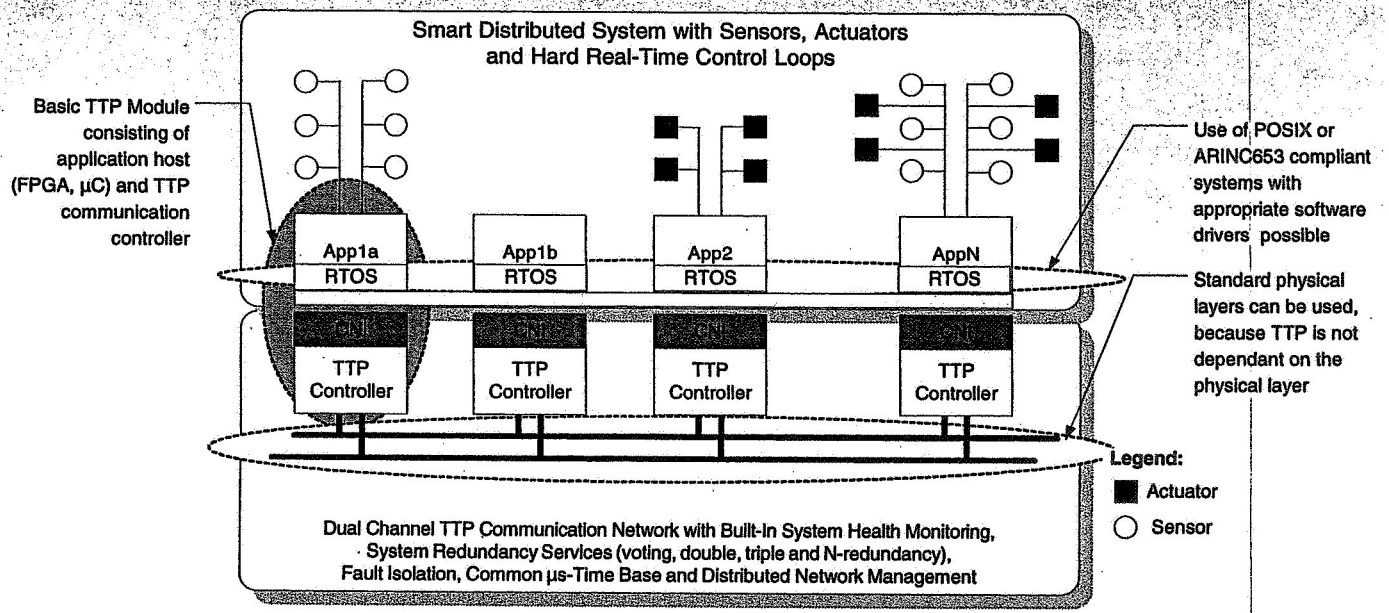
TTTech

Reduced obsolescence management costs

- Application software can be made independent of:
  - OS version (e.g. 2.0 vs. 4.0)
  - Host hardware
  - system redundancy scheme
  - Physical layer / communication speed
- TTP as a thin layer between standard components

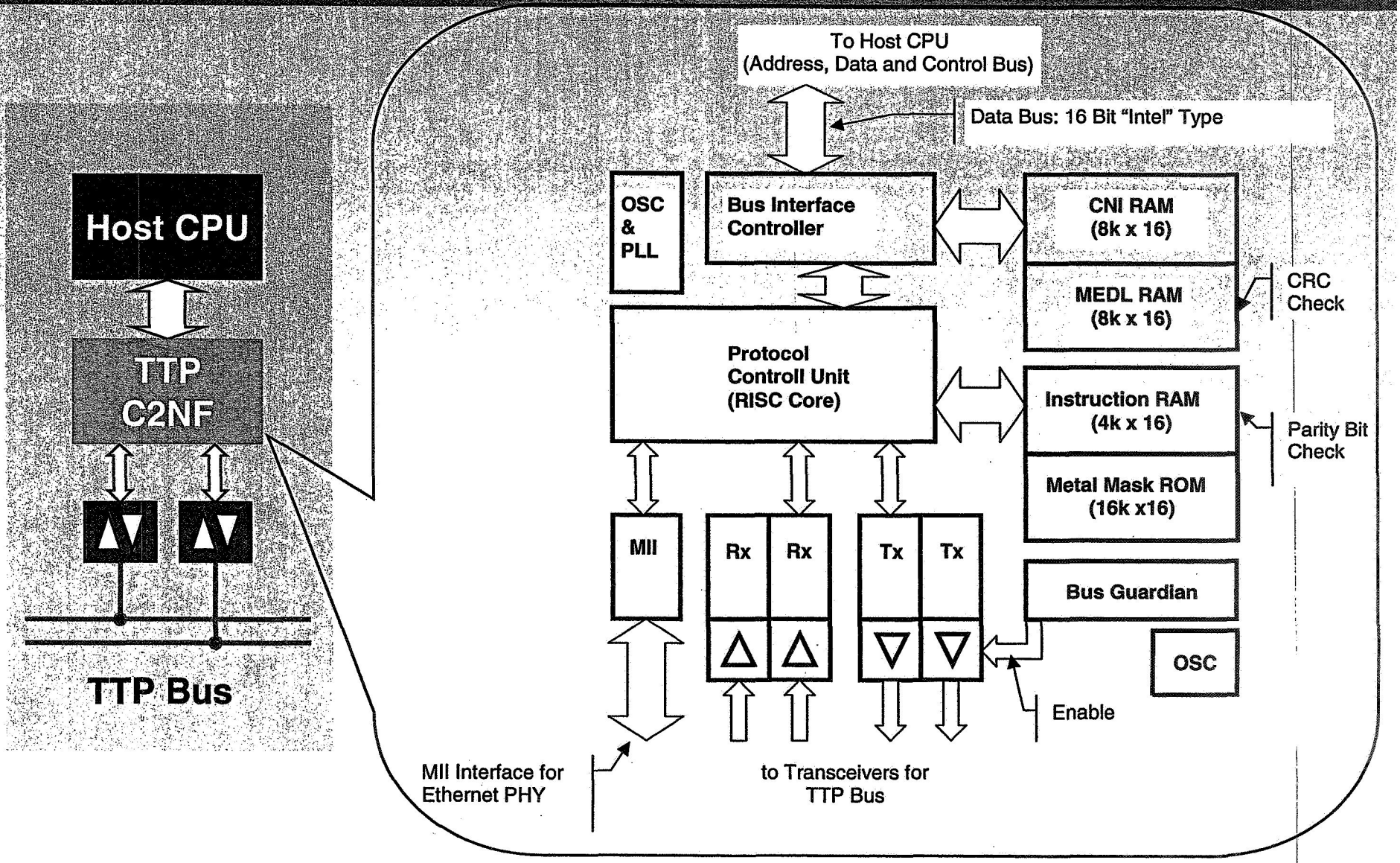






C2NF – TTTech's Chip IP for TTP Control

TTTech



C2NF = TTP Controller with Processor Unit Core

- Fulfills TTP Protocol Specification
- Proprietary processor unit (RISC)
- TTP data transmission using MFM and Manchester coding
- MII interface for high speed Physical Layer
- 16 bit non-multiplexed host CPU interface
- 16k x 16 instruction ROM
- 16k x 16 MEDL and CNI SRAM
- 4k x 16 instruction SRAM

Notes:

MEDL = Message Descriptor List ; configuration register

CNI = Controller Network Interface ; dual ported RAM

Project: Space application

- Available standard controllers (e.g. AS8202NF by austriamicrosystems) are not qualified for space use
- C2NF implementation must be radiation tolerant
- Selected FPGA family RTAX 2000 (Actel)
- Major issues: limited RAM size, no PLLs

Study

- Evaluate required restrictions to original C2NF model
- Preliminary assumption: reduction of message buffer is necessary
- Evaluate impact to development tools and TTP network performance
- Target prototype with AX2000 devices (considering RT impacts)

C2NF – Rad Hard Implementation

TTTech

TBD. – work in progress

Here FPGA implementation study results will be introduced if available at the time of the conference.

Future Outlook: Technology Development

TTTech

Today:

- Specification stable since 2002
- Chips available since 1998

Tomorrow:

- More communication speed
- Advanced distributed services
- Improved support for IVHM

Note: IVHM = Integrated Vehicle Health Management

Future Outlook: Industry Applications

TTTech

Today:

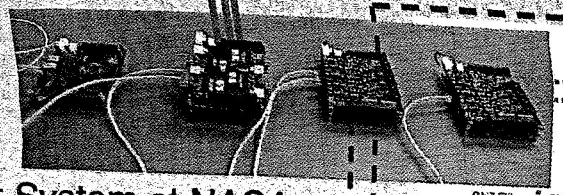
- Control systems for Boeing 787
- Control systems for Airbus A380
- Control systems for military aircraft (F-16, M-346)
- Control systems for DARPA Grand Challenge (Red Team)

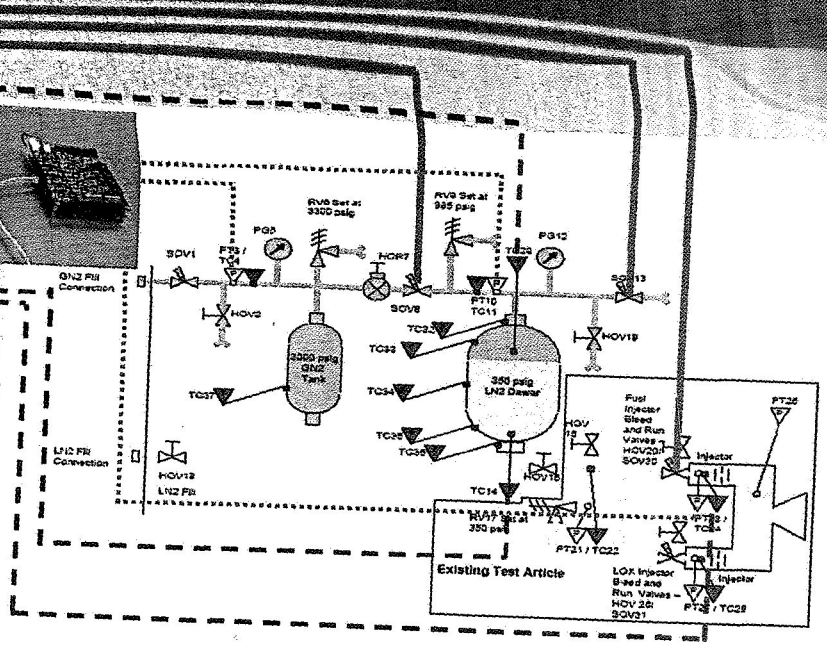
Tomorrow:

- Design wins of new „more electric“ aircraft (commercial/military)
- Design wins of new unmanned systems (UAV/UUV/UGVs)
- Design wins of new space systems

Future Outlook: Space Application

TTTech





Today:

- Aerospace Development System at NASA MSFC
  - TTP is backbone of a modular distributed real time control system
  - Incorporates IEEE 1453.4 IEEE Standard for A Smart Transducer Interface for Sensors and Actuators—Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats
    - Plug-n-play sensors
  - Stackable function boards to tailor functionality at distributed modules
- Tested as controller for simulated pressure fed rocket engine – prototype for methane/lOX engine

Future:

- Continued refinement of development system for space applications through partnerships with Johnson Space Center and Kennedy Space Center
- Candidate for use in control of critical subsystems in future launch vehicles and manned spacecraft
- Candidate for Test Stand Operation – i.e. Methane/LOX engine hotfire testing at MSFC
- Candidate for Lunar missions – robotic and control of subsystems for lunar base infrastructure